(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
14. August 2003 (14.08.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/067438 A2

(51) Internationale Patentklassifikation[7]: G06F 12/14

(21) Internationales Aktenzeichen: PCT/DE03/00184

(22) Internationales Anmeldedatum:
23. Januar 2003 (23.01.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 05 316.2 8. Februar 2002 (08.02.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **GAMMEL, Berndt, M.** [DE/DE]; Dr.-Brenner-Str. 16, 85570 Markt Schwaben (DE). **KÜNEMUND, Thomas** [DE/DE]; Lindwurmstr. 129c, 80337 München (DE). **SEDLAK, Holger** [DE/DE]; Kramergasse 2a, 82054 Sauerlach (DE).

(74) Anwalt: **EPPING, HERMANN & FISCHER**; Ridlerstrasse 55, 80339 München (DE).

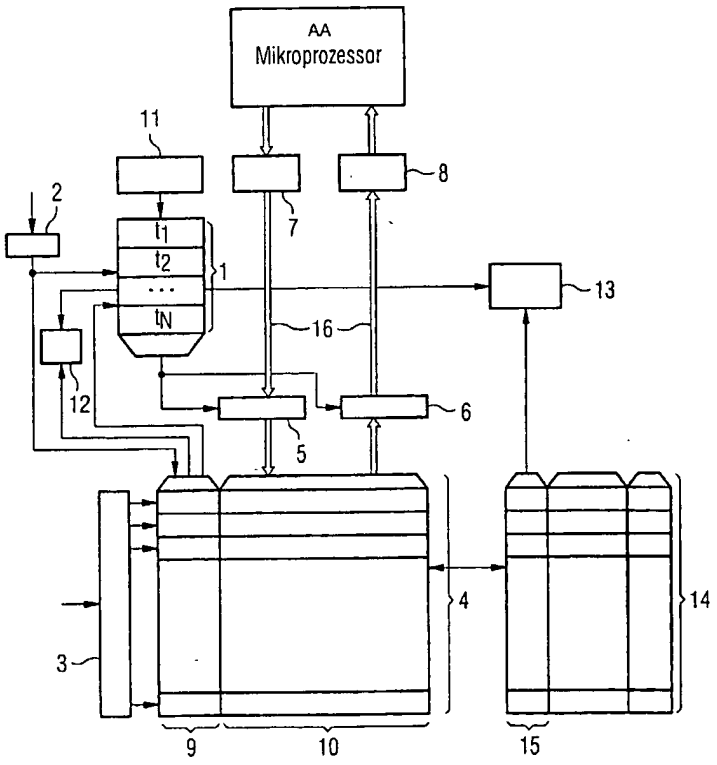
(81) Bestimmungsstaaten *(national)*: BR, CA, CN, IL, IN, JP, KR, MX, RU, UA, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: CODE MANAGEMENT DEVICE FOR THE ENCODED STORAGE OF DIGITAL DATA WORDS

(54) Bezeichnung: SCHLÜSSELMANAGEMENTEINRICHTUNG UND VERFAHREN ZUR VERSCHLÜSSELTEN ABLAGE VON DIGITALEN DATENWÖRTERN



AA MICROPROCESSOR

(57) Abstract: The invention relates to a code management device for electronic memories and to a method for the encoded storage of digital data words in electronic memories, according to which every stored data word is encoded with a digital code that can be different from another digital code of another stored data word.

(57) Zusammenfassung: Die Erfindung betrifft eine Schlüsselmanagementeinrichtung für elektronische Speicher und ein Verfahren zur verschlüsselten Ablage von digitalen Datenworten in elektronischen Speichern, bei dem jedes gespeicherte Datenwort mit einem digitalen Schlüsselwort verschlüsselt ist, das von einem anderen digitalen Schlüsselwort eines anderen gespeicherten Datenwortes verschieden sein kann.

WO 03/067438 A2

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Schlüsselmanagementeinrichtung und Verfahren zur verschlüsselten Ablage von digitalen Datenwörtern.

Die Erfindung betrifft eine Schlüsselmanagementeinrichtung für elektronische Speicher und ein Verfahren zur verschlüsselten Ablage von digitalen Datenwörtern in elektronischen Speichern.

Bei elektronischen Speichern werden grundsätzlich zwei verschiedene Speichertypen unterschieden. Zum einem sind dies flüchtige Speicher wie RAM und Speicher mit kurzen Zugriffszeiten, die oftmals als Zwischenspeicher verwendet werden wie Cash-Speicher, zum anderen sind dies nichtflüchtige Speicher wie ROM oder EEPROM. All diesen Speichern ist gemeinsam, daß sie aus regulären, regelmäßigen Strukturen aufgebaut sind und daher leicht analysierbar oder manipulierbar sind.

Bei sicherheitskritischen Anwendungen werden aus diesem Grund, die elektronisch in den Speichern abgelegten Daten, durch geeignete kryptographische Verschlüsselungsmethoden geschützt, das heißt, die Daten werden verschlüsselt abgespeichert.

Der Zugriff auf verschlüsselte Informationen in den Speichern, ist zwangsläufig von höheren Zugriffszeiten zu den Daten begleitet, da die Daten beim Einlesen in den Speicher verschlüsselt werden müssen und beim Auslesen aus dem Speicher entschlüsselt werden müssen. Bei externen Speichermedien wie Chipkarten ist dies unumgänglich und wird in Kauf genommen. Speicher aber, deren Aufgabe es ist, Daten zwischenzuspeichern und schnell wieder zur Verfügung zu stellen, wie Zwischenspeicher, Caches oder ähnliche, können aufgrund ihrer Aufgabe keine aufwendigen und zeitraubenden Verschlüsselungsverfahren anwenden.

Die Offenlegungsschriften WO 01/54083 A1 und WO 01/53931 A3 schlagen für solche Speicheranwendungen temporär gültige Schlüsselworte vor, mit denen alle Datenworte mittels eines einfachen Verfahrens verschlüsselt werden und so verschlüsselt in diesem Speicher abgelegt sind. Dabei kann, je nach Sicherheitsanforderung, der Schlüssel mit höherer oder niedrigerer Frequenz gewechselt bzw. erneuert werden.

Nach der Aktualisierung eines Schlüsselwortes ist der sich im Speicher befindliche und mit dem vorhergehenden Schlüsselwort verschlüsselte Dateninhalt nicht entschlüsselbar. Um dies zu vermeiden, muß der Speicherinhalt bei einem Wechsel des Schlüsselwortes neu verschlüsselt und wieder in den Speicher geladen werden. Sind die Sicherheitsanforderungen hoch und wird aus diesem Grund der Schlüssel häufig gewechselt, führt dies zu spürbaren Performance-Einbrüchen. Es ergibt sich also ein Konflikt zwischen Sicherheit und Performance.

Der Erfindung liegt die Aufgabe zugrunde, auch bei häufigem Schlüsselwechsel, aufgrund eines hohen Sicherheitsbedarfs, eine hohe Performance und damit einhergehend kurze Zugriffszeiten zu den Daten sicherzustellen.

Diese Aufgabe wird durch die in Patentanspruch 1 und 8 vorgeschlagenen Maßnahmen gelöst.

Dabei stehen zeitgleich eine Vielzahl von Schlüsselworten zur Verschlüsselung sensibler Daten zur Verfügung. Beim Einlesen eines Datenwortes in einen Speicher, wählt eine Schlüsselauswahleinrichtung nach einem vorgegebenen Algorithmus einen aktiven Schlüssel aus einem Schlüsselwortspeicher aus. Dieser wird dann ebenso, wie ein damit verschlüsseltes Datenwort mit einer eindeutigen Markierung versehen. Das Datenwort wird mittels einer Verschlüsselungseinrichtung verschlüsselt und in dem Speicher abgelegt. Parallel zu der Ablage des verschlüsselten Datenwortes erfolgt die Ablage der Markierung. Die Markierung stellt dabei eine eindeutige Verbindung zwi-

schen verschlüsseltem Datenwort und dem zugehörigen Schlüsselwort her. Für jeden weiteren Speichervorgang kann nun ein anderes Schlüsselwort gewählt werden. Vorteilhaft an diesem Verfahren ist, daß für jedem Speichervorgang ein neues Schlüsselwort gewählt werden kann und damit eine höchste sinnvolle Frequenz zur Schlüsselworterneuerung erreicht ist.

Soll nun ein bestimmtes Datenwort ausgelesen werden, so ermittelt eine erste Vergleichseinrichtung über die Markierung des verschlüsselten Datenwortes das geeignete Schlüsselwort im Schlüsselwortspeicher und führt dieses Schlüsselwort einer Entschlüsselungseinrichtung zu. Dies hat zur Folge, daß die Speicherinhalte mit jeweils unterschiedlichen Schlüsselworten verschlüsselt sind und diese Schlüsselworte bei einem Entschlüsselungsvorgang stets zur Verfügung stehen. Bei einer Erneuerung eines Schlüsselwortes, muß nicht der gesamte Speicher neu eingelesen und verschlüsselt werden, sondern bleibt stets entschlüsselbar.

Eine vorteilhafte Erweiterung der Erfindung stellt die in Patentanspruch 8 dargestellte und beschriebene Umsetzung einer Gültigkeitsdauer der einzelnen Schlüsselworte dar. Dabei werden Schlüsselworte, die bereits eine definierte Zeit in dem Schlüsselwortspeicher bereitstehen, nicht mehr für neue Verschlüsselungsvorgänge herangezogen. Diese Schlüsselworte werden erst dann gelöscht, wenn alle mit ihnen verschlüsselte Datenworte aus dem Speicher ausgelesen, bzw. entfernt wurden.

In weiteren vorteilhaften Ausgestaltungen der Erfindung werden die Verschlüsselungseinheit und die Entschlüsselungseinheit zu einer gemeinsamen Ver- und Entschlüsselungseinheit zusammengefaßt.

Des weiteren ist es vorteilhaft, den Eingang der Schlüsselmanagementeinrichtung und den Ausgang der Schlüsselmanagementeinrichtung durch einen bidirektionalen Datenbus zu realisieren.

Eine weitere vorteilhafte Ausgestaltung der Erfindung sieht für einen Zwischenspeicher, dessen Inhalte mit der zentralen Speichereinheit korrespondieren, eine weitere bzw. eine zweite Vergleichseinrichtung vor. Diese prüft den Speicherinhalt des Zwischenspeichers auf die Existenz verschlüsselter Datenworte mit Markierungen bereits aus dem Pool entfernter Schlüsselwörter. Wird die Existenz eines solchen verschlüsselten Datenwortes festgestellt, wird es aus dem Zwischenspeicher entfernt.

Eine weitere vorteilhafte Ausgestaltung sieht vor, alle diejenigen verschlüsselten Datenworte des Zwischenspeichers für den Fall in den Hauptspeicher zurückzuschreiben und neu zu verschlüsseln, bei dem die Markierungen der verschlüsselten Datenworte auf Schlüssel verweisen, die nicht mehr für neue Verschlüsselungsvorgänge herangezogen werden und aus diesem Grund bald nicht mehr im Schlüsselspeicher zur Entschlüsselung zur Verfügung stehen werden. Vorteilhaft ist dabei, daß Inhalte des Zwischenspeichers nicht allein durch ein ungeprüftes Löschen der Schlüsselworte ihre Gültigkeit verlieren.

Im Weiteren sei die Erfindung anhand eines Ausführungsbeispiels, unter Bezugnahme auf die Figur näher beschrieben.

Die Figur zeigt eine erfindungsgemäße Schlüsselmanagementeinrichtung für elektronische Speicher mit ihren einzelnen Komponenten und deren Verbindungen zueinander als Prinzipdarstellung.

Ein Schlüsselwortspeicher 1 enthält alle zur Verfügung stehenden Schlüsselworte t_1 bis t_n. Die Versorgung des Schlüsselwortspeichers 1 mit neuen Schlüsselworten wird über einen zweiten Eingang 11, sichergestellt.

Eine Schlüsselauswahleinrichtung 2 wählt bei einem Speichervorgang einen aktiven Schlüssel, aus dem sich im Schlüssel-

wortspeicher 1 befindlichen Schlüsselwortpool aus, woraufhin dieser in der Verschlüsselungseinheit 5 zur Verschlüsselung des Datenworts herangezogen wird. Dabei wird ein verschlüsseltes Datenwort mit der Markierung seines Schlüssels in einer zentralen Speichereinheit 4 abgelegt. Es erfolgt dabei die Ablage des verschlüsselten Datenwortes in einer zweiten Speicherzelle, und die Ablage der Markierung des verschlüsselten Datenwortes in einer ersten Speicherzelle der zentralen Speichereinheit 4. Zur Adressierung der Speicherzellen wird eine Adressiereinheit 3 herangezogen.

Ein Auslesevorgang aus dem Speicher erfolgt in umgekehrter Weise. Dabei wird aus der ersten Speicherzelle 9 der zentralen Speichereinheit 4 die Markierung des verschlüsselten Datenwortes ausgelesen und mit einer ersten Vergleichseinrichtung 12 das passende Schlüsselwort aus dem Schlüsselwortspeicher ermittelt. Eine Entschlüsselungseinheit 6, entschlüsselt dann mit dem ausgewählten Schlüsselwort die gespeicherte Information.

Ein weiteres Beispiel beschreibt die Anwendung der Erfindung bei Zwischenspeichern, sogenannten Cache-Speichern. Bei Cache-Speichern müssen alle verschlüsselten Datenworte aus dem Speicher entfernt werden, deren Markierung auf einen Schlüssel verweist, der zum Entschlüsseln nicht mehr zur Verfügung steht. Um dies durchzuführen, kann ein Löschmechanismus implementiert werden, der diese im Cache-Speicher eingetragenen verschlüsselten Datenworte als ungültig markiert. Zur Realisierung eines solchen Löschmechanismus werden die Speicherfelder, in denen die Markierungen der verschlüsselten Datenworte abgelegt sind, als "content addressable memory" ausgelegt. Bevor ein Schlüsselwort aus dem Schlüsselwortspeicher gelöscht wird, wird dann in diesem "content addressable memory" nach der Markierung dieses Schlüssels gesucht. Dabei sorgt eine Schaltung dafür, daß jedes Datenwort mit der Markierung des Schlüssels, als ungültig markiert wird.

Es ist auch möglich, die Dateneinträge des Cache-Speichers in den zugrundeliegenden Hauptspeicher zurückzuschreiben. Damit kann die Konsistenz zwischen Cache- und Hauptspeicher sichergestellt werden.

Es ist zweckmäßig, die Suche nach der Markierung so auszulegen, daß bei der Suche die gefundenen Markierungen und die dazugehörigen verschlüsselten Datenworte gesucht werden und der Schlüssel aus dem Schlüsselwortspeicher erst dann gelöscht wird, wenn kein dazugehöriges Datenwort mehr in dem Cache-Speicher vorhanden ist.

Zur Steuerung der beschriebenen Abläufe kann ein Register an die erfindungsgemäße Schlüsselmanagementeinrichtung angeschlossen werden, welches die Informationen für jede einzelne erforderliche Aktion enthält. Dazu gehören:

a) der Vergleich bzw. die Suche nach einer bestimmten Markierung eines bestimmten Schlüsselwortes,

b) im Falle der Verwendung der Erfindung bei einem Cache-Speicher, das Ungültigsetzen von verschlüsselten Datenworten mit der Markierung eines nicht mehr gültigen Schlüsselwortes,

c) eine Funktion, mit der das Zurückschreiben aus dem Cache-Speicher in den Hauptspeicher angestoßen werden kann,

d) eine Angabe darüber, ob und wenn ja, wie viele verschlüsselte Datenworte mit Markierungen, die auf nicht gültige oder nicht mehr gültige Schlüsselworte verweisen, existieren und

e) die Informationen zur Verfügung zu stellen, die zum Zurückschreiben aus einem Cache erforderlich sind.

Patentansprüche

1) Schlüsselmanagementeinrichtung für elektronische Speicher, die umfaßt:

- einen Schlüsselwortspeicher (1) zum gleichzeitigen Speichern mehrerer digitaler Schlüsselworte (1) (t_1 bis t_n),

- eine Schlüsselauswahleinrichtung (2), die mit dem Schlüsselwortspeicher (1) verbunden ist,

- eine zentrale Speichereinheit (4), die erste Speicherzellen (9) zum Speichern von Markierungen und zweite Speicherzellen (10) zum Speichern von verschlüsselten Datenworten enthält,

- eine Adressiereinheit (3) zur Adressierung der Speicherzellen einer zentralen Speichereinheit (4),

- eine Verschlüsselungseinheit (5), die mit den Speicherzellen (10) und dem Schlüsselwortspeicher (1) verbunden ist,

- eine Entschlüsselungseinheit (6), die mit den Speicherzellen (10) und dem Schlüsselwortspeicher (1) verbunden ist,

wobei die Schlüsselauswahleinrichtung (2) eine Zuordnung zwischen einem im Schlüsselwortspeicher (1) gespeicherten Schlüsselwort und den mit diesem Schlüsselwort verschlüsseltem Datenwort erzeugt.

2) Schlüsselmanagementeinrichtung nach Patentanspruch 1, dadurch gekennzeichnet, daß ein Eingang (7) für die zu speichernden Datenworte mit der Verschlüsselungseinheit (5) verbunden ist und ein Ausgang (8), für die auszulesenden Datenworte, mit der Entschlüsselungseinheit (6)

verbunden ist, und einem zweiten Eingang (11) über den die digitalen Schlüsselworte dem Schlüsselwortspeicher (1) zugeführt werden.

3) Schlüsselmanagementeinrichtung nach Patentanspruch 1, dadurch gekennzeichnet, daß die Verschlüsselungseinheit (5) und die Entschlüsselungseinheit (6) zu einer gemeinsamen Ver- und Entschlüsselungseinheit zusammengefaßt sind.

4) Schlüsselmanagementeinrichtung nach einem der vorhergehenden Patentansprüche, dadurch gekennzeichnet, daß der Eingang (7) und der Ausgang (8) durch einen bidirektionalen Datenbus (16) realisiert sind.

5) Schlüsselmanagementeinrichtung nach einem der vorhergehenden Patentansprüche, dadurch gekennzeichnet, daß eine erste Vergleichseinrichtung (12) mit dem Schlüsselwortspeicher (1) und den ersten Speicherzellen (9) der zentralen Speichereinheit (4) verbunden ist und diese die Markierungen der Schlüsselworte mit den gespeicherten Markierungen der verschlüsselten Datenworte vergleicht.

6) Schlüsselmanagementeinrichtung nach einem der vorhergehenden Patentansprüche, dadurch gekennzeichnet, daß die zentrale Speichereinheit (4) mit einem Zwischenspeicher (14) verbunden ist und die Inhalte der beiden Speicher korrespondieren.

7) Schlüsselmanagementeinrichtung nach einem der vorhergehenden Patentansprüche, dadurch gekennzeichnet, daß eine zweite Vergleichseinrichtung (13) mit dem Schlüsselwortspeicher (1) und einem Zwischenspeicher (14) und den darin befindlichen dritten Speicherzellen (15) verbunden ist und die diese Markierungen der Schlüsselworte mit den gespeicherten Markierungen der verschlüsselten Da-

tenworte vergleicht.

8) Verfahren zur verschlüsselten Ablage von digitalen Datenworten in elektronischen Speichern,

bei dem jedes zu speichernde Datenwort mit einem digitalen Schlüsselwort verschlüsselt wird,

das von einem anderen digitalen Schlüsselwort eines anderen gespeicherten Datenwortes verschieden sein kann,

für jeden Verschlüsselungsvorgang nach einer vorbestimmten Weise ein digitales Schlüsselwort aus einem Pool digitaler Schlüsselworte ausgewählt wird,

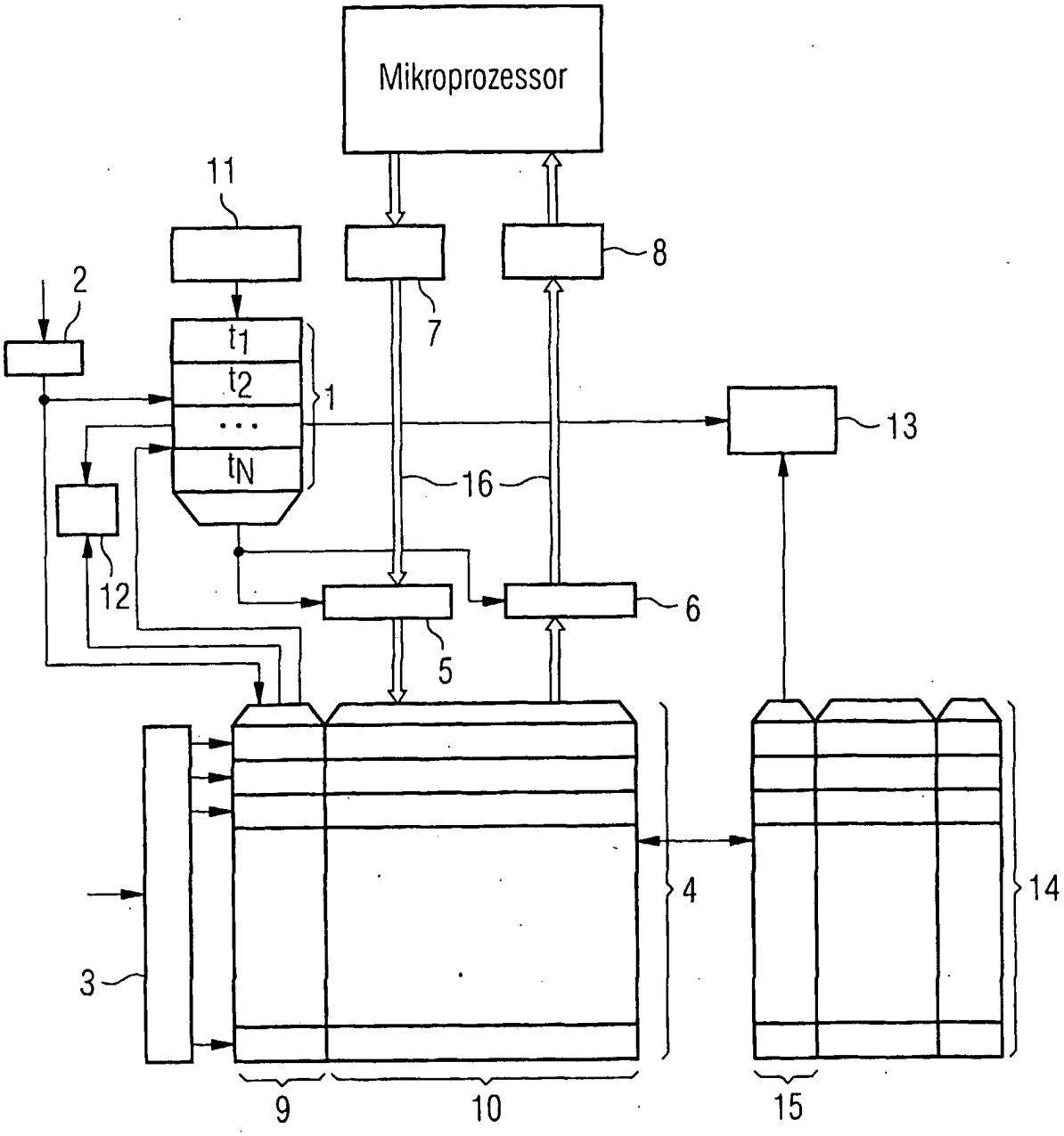
jedes digitale Schlüsselwort und jedes damit verschlüsselte Datenwort mit einer Markierung versehen wird, die das digitale Datenwort eindeutig mit einem digitalen Schlüsselwort verknüpft und

die digitalen Schlüsselworte räumlich getrennt von den verschlüsselten Datenworten gespeichert werden.

9) Verfahren nach Patentanspruch 8, bei dem ein digitales Schlüsselwort nach Ablauf einer definierten Gültigkeitsdauer nicht mehr zur Verschlüsselung ausgewählt wird und bei dem alle digitalen Schlüsselworte aus dem Pool entfernt und durch neue digitale Schlüsselwörter ersetzt werden, deren Gültigkeit abgelaufen und auf die keine Markierungen von verschlüsselten Datenwörtern verweisen.

10) Verfahren nach Patentanspruch 9, bei dem in angeschlossenen elektronischen Zwischenspeichern parallel abgelegte verschlüsselte Datenworte ungültig werden, deren Markierungen auf Schlüsselworte verweisen, die aus dem Pool entfernt wurden.

11) Verfahren nach Patentanspruch 10, bei dem in angeschlossenen elektronischen Zwischenspeichern parallel abgelegte verschlüsselte Datenworte in die zentrale Speichereinheit (4) zurückgeschrieben werden, deren Markierungen auf Schlüsselworte verweisen, deren Gültigkeit abgelaufen ist, die aber noch nicht aus dem Pool entfernt wurden.


Mikroprozessor
11
2
8
7
t1
t2
...
tN
1
13
16
12
6
5
4
14
3
9
10
15